

WHAT IS CLAIMED IS:

1 1. A method for distributing information to a plurality of conditional
2 access receivers with a plurality of different signature checking capabilities, the method
3 comprising:

4 generating a first signature over the information;
5 generating a second signature over the information;
6 sending the first and second signatures to the plurality of conditional
7 access receivers; and
8 sending the information to the plurality of conditional access receivers.

1 2. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 1, further comprising:

4 receiving the first signature associated with the information at a
5 conditional access receiver;
6 receiving the second signature associated with the information at the
7 conditional access receiver;
8 determining a signature checking capability of the conditional access
9 receiver;
10 choosing one of the first and second signatures;
11 calculating a third signature over the information; and
12 comparing the third signature to one of the first and second signatures.

1 3. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 1, further comprising:

4 generating a checksum over at least the information; and
5 sending the checksum to the plurality of conditional access receivers.

1 4. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 1, wherein the sending the first and second signatures and sending the
4 information comprise sending the same message.

1 5. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 1, wherein:

4 the plurality of conditional access receivers includes a first and second
5 conditional access receivers;

6 the first conditional access receiver uses a first signature algorithm
7 different from a second signature algorithm used by the second conditional access
8 receiver.

1 6. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 1, wherein the information comprises a software object.

1 7. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 1, wherein the information comprises authorization information.

1 8. A method for distributing information to a plurality of conditional
2 access receivers with a plurality of different signature checking capabilities, comprising:
3 receiving a first signature associated with a message at a conditional
4 access receiver;
5 receiving a second signature associated with the message at the conditional
6 access receiver;
7 choosing one of the first and second signatures;
8 calculating a third signature over the message; and
9 comparing the third signature to one of the first and second signatures.

1 9. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 8, further comprising:

4 generating the first signature over the message at a location remote to the
5 conditional access receiver;

6 generating the second signature over the message at the location remote to
7 the conditional access receiver;

8 sending the first and second signatures to the plurality of conditional
9 access receivers; and
10 sending the message to the plurality of conditional access receivers.

1 10. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 8, further comprising determining a signature checking capability of
4 the conditional access receiver.

1 11. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 8, wherein the third signature corresponds to a security level that
4 excludes one or more of the plurality of conditional access receivers from the security
5 level.

1 12. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 8, further comprising generating a checksum over at least the message.

1 13. The method for distributing information to the plurality of
2 conditional access receivers with the plurality of different signature checking capabilities
3 as recited in claim 8, further comprising:
4 calculating a fourth signature over the message; and
5 comparing the fourth signature to one of the first and second signatures.

1 14. A computer message stream embodied in at least one carrier wave
2 for providing for authentication of the computer message stream, comprising:
3 a data segment comprising an object;
4 a first signature segment comprising a first signature over the data
5 segment; and
6 a second signature segment comprising a second signature over the data
7 code segment.

1 15. The computer message stream embodied in at least one carrier
2 wave for providing for authentication of the computer message stream as recited in claim

3 14, further comprising an authorization segment comprising authorization information for
4 the object.

1 16. The computer message stream embodied in at least one carrier
2 wave for providing for authentication of the computer message stream as recited in claim
3 14, further comprising an integrity segment comprising a string characteristic of the
4 object and other portions of the computer message stream.

1 17. The computer message stream embodied in at least one carrier
2 wave for providing for authentication of the computer message stream as recited in claim
3 14, wherein the data segment is sent at a different time than at least one of the first and
4 second signature segments.

1 18. The computer message stream embodied in at least one carrier
2 wave for providing for authentication of the computer message stream as recited in claim
3 14, wherein the data segment is coupled to a first carrier wave and at least one of the first
4 and second signature segments is coupled to a second carrier wave.